

CERTAIN SIMPLE, UNSOLVABLE PROBLEMS OF
GROUP THEORY. V ^{29, 30)}

BY

WILLIAM W. BOONE

(Communicated by Prof. L. E. J. BROUWER at the meeting of November 24, 1956)

We exhibit a particular group, \mathcal{G}_T , given by a finite number of defining relations on a finite number of generators and having an unsolvable word problem: there is no recursive procedure to determine for an arbitrary product of the generators of \mathcal{G}_T whether or not this product is equal to the identity.^{3, 31)} It will be directly shown that if the word problem for \mathcal{G}_T were solvable, then a certain problem about the Universal Turing Machine [V], known in fact to be unsolvable, would be solvable.

²⁹⁾ Parts I, II, III and IV have appeared in Series A, 57, Nos. 3 and 5; 58, Nos. 2 and 5 of these Proceedings, as well as Indag. Math., 16, Nos. 3 and 5 (1954); 17, Nos. 2 and 5 (1955).

In Part I, page 234, the ninth and tenth lines following the displayed material, for both occurrences of A read D and for both occurrences of B read E. In part II, page 497, for all occurrences of M in Diagrams \mathcal{A} and \mathcal{D} read C. In Part IV, page 574, the third displayed line, for z_{α}^{iL} read \bar{z}_{α}^{iL} .¹⁹⁾

³⁰⁾ The proof of the unsolvability of the word problem contained in this and subsequent paper is *not* contained in the dissertation *Several simple unsolvable problems of group theory* related to the word problem. (See footnote 1 of Part I.) Our proof was finally completed during the period 1954–56 while in residence at the Institute for Advanced Study. We were supported in 1954–55 directly by the Institute and in 1955–56 by National Science Foundation contract G-1974. Certain improvements were evolved and preparations for publication were completed while the author held a Fulbright grant to the University of Oslo.

Our thanks are due to Professor KURT GÖDEL for his kind encouragement in these matter; certain related problems for study he has suggested we hope to deal with later. When an earlier version of Lemmas 30 and 31 was explained at a colloquium at the University of Michigan, August 3, 1956, Professor ROGER LYNDON suggested an improvement which is incorporated in our present version. We are indeed indebted to Dr. JOHN ADDISON and Dr. MICHAEL RABIN for checking many of the new details during July of 1956.

³¹⁾ What with language difficulties, we are at present totally unfamiliar with the proof of the unsolvability of the word problem by P. S. NOVIKOV now available (On the algorithmic unsolvability of word problem in group theory (in Russian), Trudy Mat. Inst. im Steklov, no. 44. Izdat. Akad. Nauk SSSR, Moscow, 1955, 143 pages) and have proceeded independently. In the Mathematical Review, 17, No. 7, page 706 (1956), A. A. MARKOV vouches for the essential correctness of NOVIKOV's proof,—describing it as based upon the unsolvability of the word problem for cancellation semi-groups [VI].

It will not be necessary to understand the results of Parts I–IV in order to follow the demonstration of this result ³²).

As was explained in Part I, page 231, if our previous argument regarding the generalized TURING Machine \mathfrak{T}_5 —that formal inverses of the symbols of \mathfrak{T}_5 are in a certain sense useless—could be carried through for a two-phase machine ⁴) analogous to \mathfrak{T}_5 , then the result would be a proof of the unsolvability of the word problem rather than the quasi-MAGNUS problem. This program can, in fact, be carried out. A major difficulty is finding an analogue of \mathfrak{T}_5 for which one can demonstrate an analogue of Theorem III, Case 2 (as is accomplished in section 15 below), but once this is done, the remaining work—while, like all these matters, cumbersome and unwieldy to explain—follows fairly naturally by the methods of Parts I–IV modified as needed.

Speaking roughly we substitute for \mathfrak{T}_5 a two-phase machine complicated by the fact that it operates simultaneously on two tapes—the scanned squares on the two tapes being identified. Ignoring complications due to the presence of symbols which are like X , l_α , and r_α of \mathfrak{T}_5 this means, *e.g.*, that where in \mathfrak{T}_5 we had the operation $S_1q_2S_3 \rightarrow q_4S_1S_3$ we shall now have the operation $S_1S'_3q_2S_3S'_1 \rightarrow S'_3S'_1q_4S_1S_3$, all primed and unprimed S 's commuting. The symmetry introduced makes deletions of the form $del(\tilde{q}_\alpha^{\text{IL}}q_\alpha^{\text{IL}})$ useless ³³).

14. *A preliminary description of $\mathfrak{G}_T^{\mathfrak{M}}$.* We specify a certain formal deductive system, \mathfrak{T}_8 . A formal deductive system ((Last line of page 232 (Part I) through the fourth line of page 233)) ³²). This system is in fact a finite presentation of \mathfrak{G}_T . In order to make our proof easier to follow, however, we do not fully reveal \mathfrak{T}_8 at once; we expose the specifications for \mathfrak{T}_8 gradually as they are needed to obtain our successive results.

\mathfrak{T}_8 —First Exhibition

\mathfrak{B}_8 : q_0, q_1, \dots, q_{n+2} (*q-symbols*).
 $d_1, d_2, \dots, d_{2u+4}$ (*d-symbols*).
 $\bar{\mathbf{a}}_\alpha$, where \mathbf{a}_α is one of the above symbols. (*Barred symbols*
— the symbol $\bar{\mathbf{a}}_\alpha$ is an $\bar{\mathbf{a}}$ -symbol).

³²) To avoid an almost word-for-word repetition of earlier material we adopt the following device. At certain points in the present text we cite between double parentheses a portion of Parts I–IV with certain changes. (It will not be necessary to understand the material to make these revisions.) At that point where the citation is made we understand the earlier text thus revised to be bodily inserted into the present material. Unless otherwise stated, the number of earlier lemmas and theorems are to acquire an asterisk (*) when thus transferred to our present work and the subscript 6 is to be replaced by 8. As a reminder of this last remark an asterisk will follow “(” where pertinent.

³³) The abstract Bulletin of American Mathematical Society, 62, p. 148 gives a reduction of the extended word problem to the word problem. An attempt to give a reduction along similar lines of the quasi-Magnus problem to the word problem led to the construction of the two-tape machine.

Before specifying \mathbb{U}_8 , we give further definitions. As exemplified above, $\mathbf{a}, \mathbf{b}, \mathbf{c}, \dots$ are variables for q and d ; $\alpha, \beta, \gamma, \dots$ for subscripts on symbols. $\mathbf{A}, \mathbf{B}, \mathbf{C}, \dots$ are to be variables for words; $\mathbf{A} \rightarrow \mathbf{B}$ is the rule whose first member is \mathbf{A} and second \mathbf{B} . *Normal* words (\hat{q} -free words) are words without occurrences of barred symbols (of q -symbols or \bar{q} -symbols). Φ and Ψ are variables for normal, \hat{q} -free words.

\mathbb{U}_8 : Operation rules satisfying the condition that $\mathbf{A} \rightarrow \mathbf{B} \in \mathbb{U}_8$ implies $\mathbf{B} \rightarrow \mathbf{A} \in \mathbb{U}_8$ and made up of three disjoint subsets:

8.1 Operations of form $\Phi q_\alpha \Psi \rightarrow \Phi' q_\beta \Psi'$ (q -shift rules).

8.2 Operations of form $\Phi \rightarrow \Psi$ (\hat{q} -less operation rules).

8.3 $\left. \begin{array}{l} 1 \rightarrow \mathbf{a}_\alpha \bar{\mathbf{a}}_\alpha \\ 1 \rightarrow \bar{\mathbf{a}}_\alpha \mathbf{a}_\alpha \\ \mathbf{a}_\alpha \bar{\mathbf{a}}_\alpha \rightarrow 1 \\ \bar{\mathbf{a}}_\alpha \mathbf{a}_\alpha \rightarrow 1 \end{array} \right\}$ where \mathbf{a}_α is any symbol of \mathfrak{Z}_8 without bar

((The sixth line following displayed material (“A proof of ...”) on page 234 (Part I) and the eight succeeding lines.²⁹))

Special words are words of the form $\Phi q_\alpha \Psi$. We let Σ and Γ be variables for special words.

((Section 3 of Part I having deleted the following. The second and fourth sentences of the first paragraph (“Forward ...” “An \mathbf{a} -shift ...”) The sentence beginning in the seventh line of page 236 (“Qualification 1: If $\mathbf{A} \rightarrow \mathbf{B} \dots$ ”). The phrase “as illustrated ... lemma 4” of lines 17–18, page 236. Lemma 4 and the sentence following. The third last line of page 236 is to be replaced by: “A q^k -shift is a q -shift such that q^k occurs in the”).

((The first paragraph of Section 4 of Part II))

LEMMA 5.1.^{**12}) For any proof in \mathfrak{T}_8 , there do not exist steps, \mathbf{C}_u and \mathbf{C}_v , such that $\hat{\mathbf{a}}^t < \hat{\mathbf{b}}^k$ in \mathbf{C}_u and $\hat{\mathbf{b}}^k < \hat{\mathbf{a}}^t$ in \mathbf{C}_v .

This lemma is clear since under the marker convention there is no operation which interchanges the positions of markers.

((Footnote 12 of Part II, — but with the second sentence replaced by: “In particular L is to be interchanged with R throughout”).)

((Section 5 of Part II with the following changes. In line 8 of page 493 for both occurrences of \mathbf{A} read \mathbf{C} and for both occurrences of \mathbf{B} read \mathbf{D} ¹⁹). In the 14th line from the bottom of page 493 replace “Qualifications 1 and 2” by “Qualification 2”. In the eleventh line of page 494 delete “and terminal”. Delete that portion of Section 5 following the statement of Theorem II*.)

((Section 6 of Part II in its entirety³⁴))

³⁴) Certain bold faced capitals may be replaced by our variables for \hat{q} -free words if desired.

15. *Proof of Theorem III* for Case 2.* To demonstrate the theorem for this case we make a notational change in the numerical subscripts on the d -symbols of \mathfrak{Z}_8 and then, in terms of this notation we further specify the operation rules of \mathfrak{U}_8 . Henceforward, instead of \mathfrak{Z}_8 and \mathfrak{U}_8 we list \mathfrak{Z}_8^+ , i.e., the symbols of \mathfrak{Z}_8 not having a bar, and \mathfrak{U}_8^+ , i.e., the operation rules of \mathfrak{U}_8 which are not insertion or deletion rules. So that the condition $\mathbf{A} \rightarrow \mathbf{B} \in \mathfrak{U}_8$ implies $\mathbf{B} \rightarrow \mathbf{A} \in \mathfrak{U}_8$ will become implicit in our notation, we write $\mathbf{A} \rightarrow \mathbf{B}$, $\mathbf{B} \rightarrow \mathbf{A}$ as $\mathbf{A} \leftrightarrow \mathbf{B}$. We always understand that the various categories of operation rules listed are disjoint from each other.

\mathfrak{Z}_8 —Second Exhibition

\mathfrak{Z}_8^+ : q_0, q_1, \dots, q_{n+2} (The q -symbols.)
 $d_1, d_2, \dots, d_{u+2}; d_{1*}, d_{2*}, \dots, d_{u+2*}$ (The d -symbols.)

Where \mathbf{A} is \hat{q} -free, \mathbf{A}_* is the word obtained from \mathbf{A} by inverting the order of symbol occurrences making up \mathbf{A} and replacing each occurrence of d_α (of \bar{d}_α) by an occurrence of $d_{\alpha*}$ (of $\bar{d}_{\alpha*}$) and vice versa.

\mathfrak{U}_8^+ : 8.1 Pairs of operation rules of form $\Phi q_\alpha \Phi_* \leftrightarrow \Psi q_\beta \Psi_*$ (The q -shifts.)

8.2 Pairs of operation rules of form $\Phi \leftrightarrow \Psi$. (The \hat{q} -less operations.) If $\Phi \rightarrow \Psi$ is $\in \mathfrak{U}_{8,2}^+$ so also is $\Phi_* \rightarrow \Psi_*$.

Since H is malcev Diagram \mathcal{J} may be rep $H(\Sigma/\Gamma)$ with full generality. We now show that for our purposes we may assume no q^t -shifts, $t \neq i$, and no \bar{q} -insertions occur in K_3 when Diagram \mathcal{J} is rep $H(\Sigma/\Gamma)$.

LEMMA 27. *If there is a malcev $H(\Sigma/\Gamma)$ such that $O_q = \text{del}(\bar{q}_\alpha^{\text{IL}} q_\alpha^{\text{IL}})$, then there is an $H^\circ(\Sigma/\Gamma)$ such that*

$$(27.1) \quad O_q^\circ = \text{del}(\bar{q}_\alpha^{\text{IL}} q_\alpha^{\text{IL}}) \text{ for a certain } i;$$

$$(27.2) \quad \text{Diagram } \mathcal{J} \text{ may be rep } H^\circ(\Sigma/\Gamma);$$

$$(27.3) \quad N_q^\circ = N_q;$$

moreover,

$$(27.4) \quad \text{When Diagram } \mathcal{J} \text{ is rep } H^\circ(\Sigma/\Gamma) \text{ no } q^t\text{-shifts, } t \neq i, \text{ and no } \bar{q}\text{-insertions occur in } K_3.$$

With only obvious changes (including an interchange of left and right) the proof of Lemma 8* (including Diagram \mathcal{B} and \mathcal{C}) constitutes a proof of this lemma.

LEMMA 28. *If there is an $H^\circ(\Sigma/\Gamma)$ such that 27.1, 27.2 and 27.4, then there is an $H^\circ(\Sigma/\Gamma)$ such that*

$$(28.1) \quad O_q^\circ = \text{del}(\bar{q}_\alpha^{\text{IL}} q_\alpha^{\text{IL}}) \text{ for a certain } i;$$

$$(28.2) \quad \text{Diagram } \mathcal{J} \text{ may be rep } H^\circ(\Sigma/\Gamma);$$

$$(28.3) \quad N_q^\circ = N_q;$$

(28.4) Where Diagram \mathcal{J} is rep $H^\diamond(\Sigma/\Gamma)$ no q^t -shifts, $t \neq i$, and no \bar{q} -insertions occur in K_3 ;

moreover,

(28.5) When Diagram \mathcal{J} is rep $H^\diamond(\Sigma/\Gamma)$ the sequence K_3 contains no operations right of the left-most \bar{q} -marker in \mathbf{E} .

With Diagram \mathcal{J} rep $H^\diamond(\Sigma/\Gamma)$ suppose \mathbf{E} is of form $\mathbf{E}'\bar{q}_6^t\mathbf{E}''$ where \mathbf{E}' is \bar{q} -free. H^\diamond is K_1 ins $(\bar{q}_\alpha^{\text{IL}}q_\alpha^{\text{IL}})K'_3O_qK''_3K_5$ where K'_3 (where K''_3) consists of the subsequence of operation of K_3 performed left (performed right) of \bar{q}^t . Since K_3 contains no q^t -shifts (27.4) clearly $\vdash^{H^\diamond} \Sigma/\Gamma$.

If \mathbf{M}, \mathbf{N} are \bar{q} -free words, $\mathbf{M} \vdash' \mathbf{N}$ means that $\mathbf{M} \vdash_{\mathfrak{g}} \mathbf{N}$ effected without the use of q -shifts, \bar{q} -insertions, or \bar{q} -deletions.

LEMMA 29. The relation \vdash' is an equivalence relation on the class of \bar{q} -free words compatible with the operation of juxtaposing representatives, under which operation these equivalence classes form a group. If $\mathbf{M} \vdash' \mathbf{N}$, then $\mathbf{M}_* \vdash' \mathbf{N}_*$.

The second sentence of the lemma follows from the condition imposed on $\mathfrak{U}_{8,2}$, i.e., the \bar{q} -less operations, in the second exhibition of \mathfrak{Z}_8 .³⁵⁾

LEMMA 30. Diagram $\mathcal{J}|\mathcal{J}$ may be rep $H^\diamond(\Sigma/\Gamma)$ with 28.1, 28.2, 28.4, and 28.5 with full generality where \mathbf{R} and \mathbf{T} are \bar{q} -free words. When this diagram is so interpreted, $\mathbf{R} \vdash' \mathbf{T}$.

The first sentence of the lemma follows from 28.4 and 28.5, \mathbf{R} being that portion of \mathbf{E} left of all the \bar{q} -markers of \mathbf{E} when Diagram \mathcal{J} is rep $H^\diamond(\Sigma/\Gamma)$. Since $1_* \vdash' \mathbf{T}\bar{\mathbf{R}}$ implies $\mathbf{R} \vdash' \mathbf{T}$, to demonstrate Lemma 30 it suffices to demonstrate Lemma 30'.

LEMMA 30'. Let Diagram $\mathcal{J}|\mathcal{J}$ be rep the $H^\diamond(\Sigma/\Gamma)$ of Lemma 30. Let the n th step of $K_3(q_\alpha^{\text{IL}}\mathbf{R}/q_\alpha^{\text{IL}}\mathbf{T})$ be $\mathbf{Y}^{(n)}q_{\beta(n)}^{\text{IL}}\mathbf{Z}^{(n)} - \mathbf{Y}^{(n)}$ and $\mathbf{Z}^{(n)}$ being \bar{q} -free — and let the n th operation of K_3 be $O^{(n)}$. Then for any n , $\mathbf{Y}^{(n)}_* \vdash' \mathbf{Z}^{(n)}\bar{\mathbf{R}}$.

For $n=1$, the lemma becomes $1_* \vdash' \mathbf{R}\bar{\mathbf{R}}$. Lemma 29 is used throughout the following argument which completes the induction step. If $^* O^{(n)}$ is a \bar{q} -less operation on $\mathbf{Y}^{(n)}$, $\mathbf{Y}^{(n)} \vdash' \mathbf{Y}^{(n+1)}$ and consequently $\mathbf{Y}^{(n)}_* \vdash' \mathbf{Y}^{(n+1)}_*$. Since $\mathbf{Z}^{(n+1)}$ is $\mathbf{Z}^{(n)}$, $\mathbf{Y}^{(n+1)}_* \vdash' \mathbf{Z}^{(n+1)}\bar{\mathbf{R}}$ — by the transitivity of \vdash' . If $O^{(n)}$ is a q^{IL} -shift assume notationally that $O^{(n)}$ is an application of the rule $Aq_\beta A_* \rightarrow Bq_\gamma B_*$, that $\mathbf{Y}^{(n)}$ is $\mathbf{Y}A$ and $\mathbf{Z}^{(n)}$ is $A_*\mathbf{Z}$ so that the induction hypothesis reads $(\mathbf{Y}A)_* \vdash' A_*\mathbf{Z}\bar{\mathbf{R}}$ or $A_*\mathbf{Y}_* \vdash' A_*\mathbf{Z}\bar{\mathbf{R}}$. Thus $\mathbf{Y}_* \vdash' \mathbf{Z}\bar{\mathbf{R}}$, $B_*\mathbf{Y}_* \vdash' B_*\mathbf{Z}\bar{\mathbf{R}}$, $(\mathbf{Y}B)_* \vdash' B_*\mathbf{Z}\bar{\mathbf{R}}$, and $\mathbf{Y}^{(n+1)}_* \vdash' \mathbf{Z}^{(n+1)}\bar{\mathbf{R}}$.

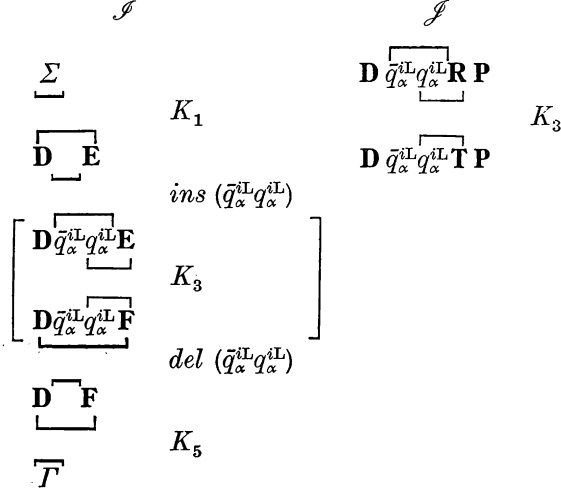
LEMMA 31. If there is an $H^\diamond(\Sigma/\Gamma)$ as described in Lemma 30, then there is an $H^1(\Sigma/\Gamma)$ such that $N_q^1 = N_q^\diamond - 1$.

³⁵⁾ The first sentence of the lemma is merely a formal statement of the fact that the symbols of \mathfrak{Z}_8 which are not q - or \bar{q} -symbols taken together with the rules of \mathfrak{U}_8 which are not q -shifts, \bar{q} -insertions, or \bar{q} -deletions constitute a finite presentation of a group.

Letting Diagram $\mathcal{J}|\mathcal{J}$ be rep $H^\circ(\Sigma/\Gamma)$, let K'_3 be the operation sequence with no \tilde{q} -insertions or -deletions and no q -shifts, such that $\lceil K'_3:\mathbf{R}/\mathbf{T}$. (Existence by Lemma 30.) Thus $\lceil K_1 \text{ ins } (\tilde{q}_\alpha^{iL} q_\alpha^{iL}) K'_3 O_q K_5:\Sigma/\Gamma$. Then H^1 is $K_1 K'_3 K_5$ since $\lceil K_1 K'_3 K_5:\Sigma/\Gamma$ and contains $N_q^\circ - 1$ \tilde{q} -deletions.

This completes the proof of Theorem III* for Case 2.

The proofs of this theorem for Cases 3 and 4 are similar* to those for Cases 1 and 2. This completes the proof of Theorem III*.



The Institute for Advanced Study, August, 1956
The University of Oslo, October, 1956